PX 400

Message

From: Brad Garlinghouse [redacted]@ripple.com]
on behalf of Brad Garlinghouse [redacted]@ripple.com> [redacted]@ripple.com]
Sent: 6/25/2019 2:36:55 PM
To: Ethan Beard [Ethan Beard <[redacted]@ripple.com>]
Subject: Re: GateHub XRP Hack Review

yes, let's discuss Thurs

On Tue, Jun 25, 2019 at 11:43 AM Ethan Beard <[redacted]@ripple.com> wrote:

I've been thinking about this a lot as part of the 'GM of XRP' hat you asked me to wear. It's also some of what I was alluding to in my weekly notes. I have a deck that lays this out and we have a 1:1 on Thursday that we can review. In the meantime, some thoughts (apologies for the length):

As GM of XRP, I think our goal is increasing the liquidity of XRP.

- We are building two technical platforms - Ripplenet and Xpring. Ripplenet has a set of developers that are building on Ripplenet and Xpring has a set of developers that are building on XRP. The tech stack, the value proposition and the business relationships are very different for these two platforms. There may be some companies that are building on both platforms but not a huge number and even in this case the approach is quite different.

- I think we should be treating all users of XRP as developers on the Xpring Platform.
- This includes both the speculative and non-speculative use case and the technical and non-technical users.
- The speculative use case can't be ignored given it's the primary use for XRP today and it's the source of liquidity for XRP. If you are an exchange trading 100s of millions of XRP a day you should have a great experience.
- The non-technical users can't be ignored as they are important parts of the XRP ecosystem. If you own $100M of XRP you should have a great experience and good info.

- The speculative developers are: exchanges, custody providers, trading platforms, traders and hodlers/whales.
- The non-speculative developers are: wallets, payment companies, users who pay/remit directly with XRP.

- We should have a tiered approach for both outreach and support with a named list of tier 1 partners that we interact with directly and long tail that we work with at scale.
- We should staff partner managers and partner engineers in region (US, EMEA, APAC) to work with our tier 1 partners. Every large partner will have an account manager who is responsible for that relationship.
- We should have developer advocates in region (US, EMEA, APAC) that does localized scaled outreach to the entire community.
- We should have scaled developer support (likely in SFO but could be regional) to support all developers.
- We will develop tools, programs, resources and content in Xpring that we will bring to market through these teams. These teams will bring feedback back to Xpring to help us build the right platform and we will work with these partners to successfully launch new features/products.
- Frankly, because Xpring has been focused on the non-speculative use cases, which are very small, it's been hard to justify building out these functions internationally. If we focus on the entire XRP ecosystem (including speculative) we have a good reason to build out these capabilities and the non-speculative users will get even better support.

- Any Ripplenet relationships, such as with Xrapid exchanges, payout partners/wallets or distribution deals such as with Metric should be handled separately. These are developers on Ripplenet.

- I'm not sure I have an opinion on where the customers/partners that we work with for Ripple's sales of XRP should live. Part of me thinks this is a straight-forward treasury function that lives in Finance. Part of me thinks it's an overall XRP liquidity function that is part of the XRP ecosystem and Xpring and we should be using it as a tool to maximize liquidity, not just to drive sales for Ripple.

I hope this makes sense - it's a lot and I've tried to distill it down. Happy to jump on a call anytime to discuss or we can talk Thursday.

-Ethan

On Tue, Jun 25, 2019 at 7:49 AM Brad Garlinghouse <[redacted]@ripple.com> wrote:

Ethan,
on the topic here: It remains confusing to me who 'owns' the account management of digital asset exchanges. I recall in a 1:1 a couple of moons ago that you had some specific thoughts on how to address? All sage counsel encouraged!

---------- Forwarded message ---------
From: **Brad Garlinghouse** <[redacted]@ripple.com>
Date: Tue, Jun 25, 2019 at 7:48 AM
Subject: Fwd: GateHub XRP Hack Review
To: Ethan Beard <[redacted]@ripple.com>, [redacted]@ripple.com>, [redacted]@ripple.com>, [redacted]@ripple.com>, [redacted]@ripple.com>, [redacted]@ripple.com>, [redacted]@ripple.com>, [redacted]@ripple.com>, Asheesh Birla <[redacted]@ripple.com>, David Schwartz <[redacted]ripple.com>, [redacted]@ripple.com>, Breanne Madigan <[redacted]@ripple.com>

Team,
I'm forwarding this to all of you given that you were all on the previous email chain with subject: "GateHub Limited Wallets" and I think useful for you all to continue to be in the loop. (and have added Breanne)

As you might guess, I think the suggestions from [redacted] have MANY issues and [redacted] appears to be looking for leadership from us in a world where he could just as easily provide that leadership / coordination - but rather than ignoring the email entirely or a dismissive reply like "thanks, we'll take a look" - I think there is value in replying with something more cogent and complete.

In the interest of efficiency: [redacted] can you take point in drafting a reply for me to send? obviously please garner input from the stakeholders on this thread.

Please let me know if questions / comments

---------- Forwarded message ---------
From: [redacted]@gatehub.net>
Date: Tue, Jun 25, 2019 at 4:28 AM
Subject: Re: [redacted] XRP Hack Review
To: [redacted]@gmail.com>
Cc: [redacted] ripple.com <[redacted]@ripple.com>, Brad Garlinghouse <[redacted]@ripple.com>, [redacted] <[redacted] com>

[redacted] thank you for your time in Slovenia and for this quick recap of the conversations we've had.

Normally I would not suggest changes to the core XRP ledger but as the attacks are getting more sophisticated I also fear that we do not have enough controls in place in order to effectively safeguard our customers. With hosted wallets, for example, we have much more control which is why we were able to successfully prevent the perpetrator to steal funds from [redacted] account.

Whitelisting and time locks would definitely be a step in the right direction. Any additional measure we can come up with will be fully supported in our Wallet for all the customers. In the meantime, we are going to re-encrypt all the wallets in the system and also implement support for regular keys.

Another thing that [redacted] didn't mention would be to standardize the way exchanges and wallet providers can effectively communicate with each other and share known suspicious addresses (blacklist) and other information.

In the attachment, you can find [redacted] open banking approach. On page 9 you'll see a thing called "Dispute & Problem Resolution". What they are doing is essentially creating a product that enables their clients (TPP's and banks) to seamlessly communicate in real-time for any disputes and suspicious activity.

A feature like this would definitely bring XRPL ahead of the curve and could also speed up investigations for law enforcement agencies.

As the payments get closer to real-time, all the supporting processes need to become faster. This will be a key challenge for anyone, including Libra.

Best regards,
[redacted]

On Tue, Jun 25, 2019 at 6:21 AM [redacted]@gmail.com> wrote:

> gday Chris and Brad,
>
> I've just returned from Slovenia and a review of the GateHub XRP Hack. My findings suggest that in addition to the hacking itself being a problem, the ability to flow stolen funds seamlessly through a combination of mixers, tumblers and decentralized exchanges to launder the proceeds is also a big vulnerability.
>
> A significant reduction in risk going forward would be to optionally allow XRP wallets to reference a whitelist of other "trusted" addresses that value could flow to and from that would preclude the ability to move funds to/from unauthorized destinations. Much like Ripple employs a config file that designates trusted validators, the same config file could (optionally) designate a list of any number of trusted wallets for sending and receiving value on the ledger. When combined with a time lock feature, the bulk of value in accounts could be safeguarded against much of the present vulnerability that has and will continue to be

exploited unless remediation is taken. I believe the feature is also a forward positioning to ensure parity/superiority to Libra.

I'd like to talk to technical folks at Ripple about what it would take to make whitelisting and time locks possible. I'd be willing to talk with [redacted] Gatehub about putting these measures in place and would even be willing to fund the further R&D around this effort in the hope that these RCL enhancements would be made available sooner rather than later. Without these enhancements, I fear that the risk/reward ratio is stacked too far in the favor of the perpetrations for GateHub to be able to effectively safeguard the 1.5M accounts and 10B associated XRP. With these measures I believe that GateHub, Ripple, and others can "green" the ecosystem and differentiate RCL/XRP from other cryptos in the marketplace.

Please ping me on [redacted] if you'd like to talk further before I broach some these ideas and get feedback from David, Arthur, [redacted] on the tech side, and Ethan on the biz/investor side of the ecosystem. Hope we can reach consensus on a plan to remediate the present vulnerability before the current hack is extended or repeated.

cheers,

[redacted]

[redacted]

[redacted]
Chief Executive Officer
[redacted]

[redacted]

[redacted] | Privacy Policy